12 November 2020

Comments by the Centre for Information Policy Leadership on China's Draft Personal Information Protection Law

The Centre for Information Policy Leadership (CIPL)[1] welcomes this opportunity to provide comments to the Standing Committee of the National People's Congress (NPC) of the People's Republic of China on the Draft Personal Information Protection Law (PIPL).

CIPL welcomes this initiative to create a robust system of data protection in China in conjunction with China's Cybersecurity Law and Draft Data Security Law. CIPL appreciates the NPC's efforts and believes this comprehensive law be a key pillar of China's data protection regime, with significantly profound influence. Our recommendations below are intended to bolster the current draft to position China well as a global leader in an increasingly and necessarily interoperable digital world. In particular, we suggest changes to avoid unnecessary negative effects on innovation and the continued development of China's digital economy.

In this submission, CIPL highlights several possible modifications of the PIPL, which it believes the NPC should consider and adopt during its review, not only to ensure China's standing in the international data protection space but also to ensure the protection of China's citizens, businesses and government data.[2]

Summary of CIPL Recommendations

This summary provides a list of the most critical recommendations contained in this submission. These recommendations are organized according to specific themes. For the full set of recommendations, organized by Article as they appear in the PIPL, please see the full comments below.

Privacy Principles and Legal Bases for Processing

- Include a legitimate interest processing ground within the PIPL.
- Make clear that if there is a change in the purpose of processing personal information that is compatible with the original purpose, organizations can process that personal information by relying on the original processing ground. If the new purpose is incompatible, a new legal ground would be required.

[1] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 83 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] Please note that the comments in this submission are based on two unofficial translations of the Personal Information Protection Law. It is possible that, as a result, we may have misunderstood the particular intent or nuance of certain issues. To the extent this is true for any particular comment, please disregard that portion of this submission.

Children's Personal Information

- Enable a risk based approached for organizations to determine whether they are processing personal information of minors in the context of mixed audience websites and must obtain consent from a guardian.

Sensitive Personal Information

- Enable a risk-based approach for processing sensitive personal information rather than providing set categories of pre-defined sensitive information.
- To the extent pre-defined categories of sensitive information are retained in the PIPL, remove financial account information and personal whereabouts from the definition and clarify how "other" forms of sensitive personal information will be defined and by whom.
- Clarify that sensitive personal information can be processed on the basis of all legal grounds for processing listed in the PIPL and that processing such information is not limited to the ground of consent – e.g. processing for protecting the life or health of an individual in an emergency situation.

International Transfers of Personal Information

- Clarify the scope of supervision required to ensure an overseas recipient of personal information from China meets the standards of protection enumerated in the PIPL.
- Explain what is required to pass the Cyberspace Administration's security assessment to transfer personal information overseas.
- Clarify whether the certifications reference in Article 38 for the transfer of personal information could enable China's participation in the APEC Cross-border Privacy Rules system and work towards joining the CBPR system in line with Article 12 of the PIPL.
- Add codes of conduct and corporate rules to the available transfer mechanisms listed in the PIPL.
- Remove the requirement to obtain consent on top of the other transfer requirements in the PIPL.

Appointing an Information Protection Officer and a Representative in China

- Revise the requirement to disclose and register the contact information of the personal information protection officer to the relevant authorities and only require registering whether such an officer has been appointed and keeping such representation accurate and up to date.
- Align the thresholds triggering the requirement to appoint a personal information protection officer with those under the Personal Information Security Specification.
- Add exemptions to the requirement to appoint a representative in China in line with those found in other privacy laws, such as the GDPR.

Risk Assessments

- Clarify that conducting an initial pre-screening of the processing activities listed in Article 54 and carrying out a full-blown risk assessment if such a screening indicates a high risk to individuals would be sufficient to meet the Article 54 requirement to conduct "advance risk assessments".

Breach Notification

- Add and elevate the harm thresholds that trigger the notification requirement to report a breach to the relevant authorities and individuals.

- Revise the requirement to notify breaches from "immediately following identification" to the most expedient time possible and without unreasonable delay but not later than a specified number of days (e.g., 30 or 45 days) after the entity becomes aware of a data breach.

Providing Data to Third Parties

- Clarify the role of third party service providers under the PIPL.

Anonymization

- Revise the definition of anonymization to reflect the more realistic standard of reasonable anonymization coupled with procedural, legal and administrative safeguards.

Publicly Available Information

- Revise the PIPL to ensure consistent rules around the use of publicly available information in line with the APEC Privacy Framework and China's Personal Information Security Specification.

Penalties

- Clarify what constitutes a "grave" unlawful act under the PIPL.

- Clarify when the fines will be a set monetary amount or percentage of revenue and that the revenue in question relates to revenue in China.

- Clarify that personal liability under Article 62 applies only to top company officers or directors who acted willfully or with gross negligence for financial gain.

Effective Date

- Specify that organizations will have two years from the date the PIPL is passed to be fully compliant with the law.

Comments

Article 3: Territorial Scope

According to Article 3, the PIPL applies to processing of personal information of individuals within the borders of China by organizations located outside of China if the purpose of the processing is (1) to provide products or services to individuals in China, (2) to analyze and evaluate the behaviors of individuals in China or (3) for other circumstances provided for by law or administrative regulations.

Given the increasingly global nature and movement of data, including such a provision in a personal information protection law provides organizations transferring or processing data abroad certainty as to which of their activities are subject to the law. However, CIPL believes that subjecting overseas organizations to the PIPL on the basis of other circumstances provided for by law or administrative regulations creates uncertainties, including potential conflicts of laws situations. CIPL recommends deleting this portion of Article 3 and elaborating on laws which trigger the extraterritorial scope of the PIPL by way of guidance in English and Mandarin from the relevant authorities as such laws are passed. This will ensure greater certainty for all stakeholders as to the responsibilities of organizations processing personal data outside of China.

Recommendation: Revise Article 3 of the PIPL to remove the provisions subjecting overseas organizations to the PIPL on the basis of other circumstances provided for by law or administrative regulations and provide further clarity on laws which trigger the PIPL's extraterritorial scope by way of guidance by the relevant authorities in English or Mandarin.

Article 6: Purpose Limitation

Article 6 of the PIPL states that personal information processing shall have a clear and reasonable purpose, and shall be limited to the minimum scope required for achieving the purpose of processing. CIPL recommends clarifying that "minimum scope" means limiting processing to the personal information that is relevant and necessary to achieving the purposes. This wording provides more clarity and will avoid confusion among organizations that are unclear about the meaning of "minimum scope", as currently included in the PIPL.

Recommendation: Clarify in Article 6 that "minimum scope" means to limit processing to personal information that is relevant and necessary to achieving the purposes.

Article 12: Participation in Formulation of International Personal Information Protection Rules

Article 12 of the PIPL provides that the State shall actively participate in the formulation of international rules on the protection of personal information, promote international exchanges and cooperation in personal information protection, and promote mutual recognition of personal information protection rules and standards with other countries, regions and international organizations.

CIPL fully supports this requirement of the PIPL and notes that the State has already started this work through developing and endorsing the APEC Privacy Framework. CIPL recommends, in line with Article 12, that China work towards formally joining the APEC Cross-Border Privacy Rules system as one method of

promoting mutual recognition of personal information protection rules and standards with other nations (see further comments under Article 38 below).

Recommendation: Work towards formally joining the APEC CBPR system in line with Article 12 of the PIPL.

Article 13: Legal Grounds for Processing Data

CIPL commends the NPC for including several legal grounds for processing personal information in the PIPL. These include processing personal information (1) on the basis of consent; (2) to enter into or perform a contract; (3) to perform statutory responsibilities or obligations; (4) to respond to public health emergencies or protect the life, health or property of individuals in emergency situations; (5) for news reporting, to conduct supervision by public opinion and other actions in the public interest; or (6) for other circumstances as stipulated by laws and administrative regulations.

CIPL notes, however, that certain forms of important personal information processing that are routine and commonplace in the modern digital society may not be able to take place within the confines of these six processing grounds alone.

Apart from consent, the processing grounds enumerated in the PIPL all relate to very specific information processing situations that constitute just a fraction of the millions of processing operations that take place every day. Moreover, while consent itself remains useful for processing data in many circumstances, there are equally many contexts in which obtaining consent is impractical, impossible, ineffective and simply not meaningful. These include, for example, (1) where there is no direct interaction with individuals, (2) where the data use is common, trivial and imposes no real privacy risk, (3) where large and repeated volumes of data are processed (seeking consent at every instance may not be feasible or may be meaningless as a result of consent fatigue) or (4) where obtaining consent would be counterproductive, such as where data is processed for network and information security or to prevent fraud or crime.

CIPL recommends including a seventh processing ground that is similar to the "legitimate interest" legal basis found in other privacy laws, including the EU GDPR, the Brazil LGPD and the Singapore PDPA.[3] The legitimate interest processing ground would enable organizations to collect and process personal information while ensuring they remain accountable for the processing and fully respect the data protection rights of individuals. Typically, such a provision requires the organization to conduct a balancing test or assessment to demonstrate that it or a third party has a legitimate interest to process the personal information and that these interests are not overridden by the rights of the individuals whose data is the subject of the processing. Moreover, this balancing test must be demonstrable to privacy enforcement authorities.

More restrictive personal information protection rules do not always equate to benefits for citizens or serve the public interest. It is important for society to allow businesses and other organizations to process personal information where necessary, for example, to detect, prevent or investigate fraud or crimes.

[3] See Article 6(1)(f) GDPR and Article 7(IX) of the Brazil LGPD. Note that Singapore has recently updated its Personal Data Protection Act to include a legitimate interest ground for processing.

For instance, it would not be appropriate to obtain consent to process personal information in the context of detecting and preventing financial crime, terrorist financing or anti-money laundering schemes. Otherwise, bad actors could simply refuse to provide consent and could carry out illegal activities undetected. Some of this activity may be covered by passing laws to tackle some forms of crime and then processing the data to comply with legal obligations but it is important to remember there are many forms of crime and they may not all be covered under legislation. Moreover, none of the other processing grounds listed in the PIPL are suitable for processing personal information in such scenarios. CIPL, therefore, recommends the inclusion of a legitimate interest processing ground that would enable such forms of important processing.

For China, including such a processing ground in the PIPL would not only bolster confidence in Chinese consumers as they communicate and engage in transactions online but would also ensure that the private sector and government can protect and enforce against criminal activities. Furthermore, the Chinese civil code includes several grounds for the exemption of liability for processing personal information, including acts carried out to safeguard public interests or the legal rights of natural persons.[4] Including a legitimate interest ground to enable processing of personal information to prevent and detect crimes and fraud would be consistent with the code and constitute an act to safeguard public interests or the legal rights of natural persons. The PIPL should build on the foundation created by the civil code and enable such forms of information processing.

It is important to note that the legitimate interest processing ground is not only essential for processing related to fraud and crime prevention. Other processing scenarios that may be addressed by such a ground include information, network, system and cybersecurity; processing personal information in employment contexts; corporate operations and due diligence; product development and enhancement; communications, marketing and business intelligence.[5] Indeed, in the growing data economy, the legitimate interest ground for processing will become increasingly important to enable a broad range of data processing activities not covered by other grounds but essential for a well-functioning digital economy and for organizations' ability to innovate. Moreover, it is important to note that due to the required risk/benefit assessments inherent in the "legitimate interest" basis for processing, which must be demonstrable to enforcement authorities, and the associated requirement to implement risk-appropriate mitigations and controls, the legitimate interest basis for processing provides a high standard of personal information protection for individuals.

With respect to the legal ground of processing within a reasonable scope for news reporting, to conduct supervision by public opinion and other actions in the public interest, it is not clear what is meant by "a reasonable scope" within the PIPL. CIPL recommends the NPC further clarify the intention behind this wording in the next iteration of the PIPL.

Recommendation: Include a legitimate interest processing ground within the PIPL and clarify what is meant by a "reasonable scope" for processing personal information for news reporting, to conduct supervision by public opinion and other actions in the public interest.

[4] See Article 1036, Presidential Decree No. 45 - The Civil Code of the People's Republic of China.
[5] See CIPL White Paper on Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR, 19 May 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf.

Article 14: Consent and Changes in Purpose of Processing

With respect to obtaining consent to process personal information, the PIPL notes that any consent shall be expressed by individuals voluntarily and explicitly on the premise of full knowledge. It is currently not clear what constitutes "full knowledge". Indeed, many individuals do not read lengthy privacy policies before engaging with online services and creating such an expectation will make it extremely difficult for organizations to demonstrate that consent was obtained in full compliance with Article 14. In addition, "full knowledge" is a subjective standard and cannot be measured uniformly across individuals. CIPL recommends that the NPC revise Article 14 to require voluntary and explicit consent in circumstances where consent is appropriate for the processing operation at hand.

Individuals cannot be expected to be fully informed about the hundreds of digital services they use on a daily basis and for many processing operations, consent is not appropriate. In such cases, individuals can be better protected via a legitimate interest processing ground (discussed above) where the burden is on the organization to balance the relevant interests, take appropriate mitigations and not engage in processing where the interests of the individual outweigh those of the organization.

Moreover, Article 14 of the PIPL notes that in case of changes to the purpose of processing personal information, consent must be re-obtained from the individual. CIPL believes that further processing of personal information for purposes that are "compatible" with the original purpose should be permitted without the need to re-obtain consent in certain circumstances. Of course, organizations may need to provide notice to the individual of the new purpose of processing, depending on the circumstances. Further processing based on "compatibility" should be allowed for future uses that are consistent with, can co-exist with, and do not undermine or negate the original purpose. These uses must be backed by strong accountability-based safeguards, including benefit and risk assessments, to ensure that new uses do not expose the individual to unwarranted increased risks or adverse impacts.

If the change in the purpose of processing is incompatible with the original purpose, a new legal ground to process the personal information would be required.

Recommendation: Revise Article 14 and remove the requirement that valid consent must be based on the premise of "full knowledge" of the individual as such a standard is too subjective to work in practice. Make clear within Article 14 that if there is a change in the purpose of processing that is compatible with the original purpose, organizations can continue to rely on the original processing ground. If the new purpose is incompatible, a new legal ground (which may include obtaining consent) would be required.

Article 15: Children's Data

In order to process Children's data under the PIPL, the personal information processor (known as a data controller in many privacy laws) must obtain consent from the guardian of a minor under the age of 14. This requirement is triggered depending on whether the personal information processor knows or should know that the personal information it handles is the personal information of a minor under the age of 14. This is relatively straightforward to determine for certain online services and products that are designed for child audiences. However, the situation becomes more complicated for mixed audience websites (i.e. if the website is not directed to children but children nonetheless use the service). Verifying the ages of all users who visit mixed audience websites to determine who is a child or not to comply with the

requirement to obtain consent from a guardian for minors would create a huge burden on organizations. In addition, it would require the collection of even more personal information such as identity documents, which would be counter to the PIPL's principle of limiting processing to the minimum scope required for achieving the purpose. Moreover, age gating mechanisms that require users to self-report ages are not foolproof as children can lie to bypass these restrictions.

CIPL recommends that the PIPL revise Article 15 to enable personal information processors to conduct a contextual determination as to whether they are likely processing the personal information of minors through an appropriate risk-based test. This can include considering factors such as the nature of the online service/product offered, the accessibility of the service, the potential attractiveness of the service to children and whether children have been attracted to similar or competing services, whether the registration process for a website/service reflects an assumption that users are above the age of 14, etc.

Such an approach is consistent with the requirement of obtaining consent where a personal information processor "should" know that it is handling the personal information of a minor. Moreover, this approach will ensure that personal information processors obtain consent from the guardians of minors without necessitating the verification of all users' ages and the collection of further information to facilitate such verification.

Recommendation: Enable personal information processors to make a contextual determination based on a number of factors to determine whether they are processing the personal information of minors in order to meet the requirements of Article 15 for mixed audience websites and services.

Article 21: Joint Personal Information Processors

Article 21 of the PIPL states that if personal information processors jointly process personal information and infringe upon the rights and interests of individuals, they shall bear joint and several liabilities in accordance with the law.

It is important to consider that joint personal information processors may play very different roles with respect to the data they are processing. As such, joint responsibility should not imply joint and several liability as one of the personal information processors may in fact carry out the majority or main processing operations. Liability levels should be assessed with regard to the context of the processing operation, the circumstances of the case and which processing activity infringed upon the rights and interests of the individual. CIPL recommends that the NPC revise Article 21 of the PIPL to state that if joint personal information processors infringe upon the rights and interests of individuals through their activities, they bear joint liability in accordance with the law and the relevant circumstances.

Moreover, Article 65 of the PIPL states that a personal information processor that is able to prove it is not at fault may be relieved or exempted from liability. This would support revising Article 21 in line with the above.

Recommendation: Revise Article 21 to make clear that the level of joint liability for joint personal information processors should be premised on the context and circumstances of the processing.

Article 23: Change in Purpose of Processing following Merger, Split or Other Reasons

The PIPL provides that if the recipient of personal information following a merger or split changes the original purpose or method of processing, it shall inform individuals and obtain their consent again in accordance with the provisions of the PIPL. CIPL would like to highlight that if the recipient of the data changes the purpose of processing to one that is compatible with the original processing, it should not need to re-obtain consent. As noted above, if the change in the purpose of processing is incompatible with the original purpose, a new legal ground to process the personal information would be required.

Recommendation: Revise Article 23 to clarify that in a merger or split, the recipient of personal information only needs to rely on a new legal ground to process data if the new purpose for using the data is incompatible with the original. This could include re-obtaining consent or relying on a different legal basis for processing.

Article 24: Provision of Personal Information to Third Parties

Article 24 of the PIPL notes that if a personal information processor provides personal information to a third party, it shall inform individuals of the third party's identity, contact information, the processing purpose and method, and types of personal information. The personal information processor must also obtain the specific consent of the individual.

It is important to highlight that in certain circumstances, an organization should not be required to obtain separate consent to provide information to a third party. For example, if processing data for the performance of a contract in the context of an online shopping transaction, it may be essential to provide the individual's name and address to a third party delivery service to deliver the product to the individual.

Moreover, it may not always be feasible to obtain consent from the individual. For example, if the personal information processor needs to transfer financial account information to tax authorities because there is a suspicion of tax fraud, it would be counterproductive to obtain consent from the individual.

Moreover, many companies use third party service providers to process personal data for data analytics and advertising purposes. Requiring separate consent to engage in such routine and common data processing activities will create major difficulties for organizations and increase costs considerably, including for individuals that currently enjoy many online services for free. To avoid such situations, CIPL recommends the inclusion of a legitimate interest ground for processing in the PIPL (see pages 5-6 above).

Furthermore, the scope of the third party recipients' obligations are not clear once they receive the data. Many third parties will be service providers acting on behalf of the personal information processor. The PIPL does not appear to distinguish between personal information providers, known as data controllers in some other privacy laws, and third party service providers. CIPL recommends that the NPC clarify the role of third party service providers under the PIPL (see further comments below on page 24).

Recommendation: Revise Article 24 to account for scenarios where an organization may not need to obtain separate consent to provide information to a third party. Clarify the role of third party service providers under the PIPL.

Article 25: Automated Decision-Making

Article 25 of the PIPL provides that when using personal information to conduct automated decision-making, personal information processors shall guarantee the transparency of their decision-making and provide a right to individuals to refuse to be subject to automated decision-making.

The purpose of this Article is to protect consumers from unfair discrimination or negative impacts resulting from automate decision-making. While CIPL understands the need for guardrails with respect to certain types of automated decisions, it believes that the PIPL should exclude business-to-business automated decisions analyzing risk and credit ratings from the scope of Article 25. Such analyses are beneficial to improving commercial efficiency and in the public interest. As such, automated decision around credit in the B2B contexts should not be subject to a right to refuse.

Recommendation: Revise Article 25 of the PIPL to carve out business-to-business automated decisions analyzing risk and credit ratings from its scope.

Article 28: Processing Disclosed Personal Information

The PIPL notes that when processing already published personal information, personal information processors shall conform to the purposes for which such personal information was published. If the processing exceeds the reasonable scope related to said purposes, the personal information processor must notify the user and obtain their consent.

China, as an APEC member economy, has endorsed the APEC Privacy Framework.[6] Part II of the Framework notes that it has limited application to publicly available information. It states that notice and choice requirements are often superfluous where the information is already publicly available and the personal information controller does not collect information directly from the individuals concerned. The Framework lists information in publicly available government records or news items broadcast or published by news media as examples of publicly available information.

Moreover, under Article 5.6 of the Personal Information Security Specification,[7] personal information gathered from legitimate and publicly available sources, such as news reports or governmental sources does not require consent to use the data to be obtained from individuals.

CIPL recommends that the NPC revise Article 28 of the PIPL in line with the APEC Privacy Framework and the Personal Information Security Specification.

[6] The APEC Privacy Framework was developed by the 21 APEC member economies and was initially finalized in 2005. See APEC Privacy Framework, available at https://www.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf. Portions of the Framework were updated in 2015 and draw upon concepts introduced into the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980, updated in 2013) with due consideration for the different legal features and context of the APEC region https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015).

[7] See Article 5.6 (h) Exceptions to Consent, Information security technology – Personal information security specification, National Standard of the People's Republic of China, GB/T 35273-2020.

Recommendation: Revise Article 28 of the PIPL to ensure consistent rules around the use of publicly available information in line with the APEC Privacy Framework and China's Personal Information Security Specification.

Article 29: Sensitive Data

Under the PIPL, sensitive personal information is defined as personal information that, once leaked or illegally used, may lead to personal discrimination or serious harm to personal and property safety, including race, nationality, religious belief, personal biological features, medical history, health, financial account, personal whereabouts and other information.

CIPL does not recommend establishing a category of pre-identified "sensitive personal information", as sensitivity of processing and information is very much context driven. Processing a particular category of personal information may not carry the same risks in all processing contexts. Instead, we recommend a risk-based approach to privacy protection that requires organizations to subject all their processing activities to a risk analysis and requires them to establish mitigations and controls appropriate to the actual risks involved. This does not mean that the law cannot include examples of what kinds of personal information might be particularly sensitive but such examples should be treated as guidelines to take into account when conducting a context-specific risk assessment rather than as automatic and invariable triggers of heightened requirements or limitations on the use of such personal information. However, to the extent that the NPC decides to include such a category in its law, CIPL has some concerns around the PIPL's definition of sensitive personal information.

The definition currently includes financial account information and personal whereabouts as types of sensitive information. Such types of personal information are regularly processed by personal information processors and including them in the definition would hinder many common processing operations. For example, workplaces often process financial account information for payroll and salary purposes. Financial account information is also processed in the context of fraud prevention. Personal whereabouts are regularly processed to deliver various forms of location-based services, including rideshare and taxi services, GPS and map applications and weather forecast information. Requiring consent from individuals to process such information may prove overly burdensome for organizations and may raise concerns of consent fatigue among individuals. CIPL recommends removing financial account information and personal whereabouts from the definition of sensitive personal information (to the extent this concept is retained in the law).

Moreover, the definition includes an open-ended category of "other information". It is not currently clear how "other information" will be defined and by whom. This has the potential to create legal uncertainty and lead to unrealistic expectations on organizations to cease processing existing personal information that is subsequently deemed to be sensitive and to seek consent from individuals. CIPL recommends that the NPC explain in the PIPL how such "other information" may be determined and by which agency. In addition, the PIPL should provide for a public consultation process to allow for proper notice and stakeholder input before further categories of personal information are deemed sensitive.

Recommendation: Revise the PIPL to enable a risk-based approach for processing sensitive personal information rather than providing set categories of pre-defined sensitive information. To the extent such pre-defined categories are retained in the PIPL, remove financial account information and personal

whereabouts from the definition. Moreover, clarify how other sensitive personal information will be defined and by which agency. Before adding further categories of sensitive personal information within the scope of the PIPL, a public consultation process should be undertaken with all relevant stakeholders.

Article 30: Consent to Process Sensitive Personal Information

Article 30 of the PIPL states that where the processing of sensitive personal information is subject to consent, personal information processors shall obtain separate consent of individuals.

It is not clear whether other legal bases other than consent can be used to process sensitive personal information. Firstly, Article 30 states that where processing of sensitive personal information is subject to consent, separate consent must be obtained. What does this mean where the first instance of processing sensitive personal information is based on another ground such as processing for protecting the life or health of an individual in an emergency situation? A personal information processor should be able to rely on that ground alone without the need to obtain any consent from the individual.

Moreover, it is important to highlight that obtaining consent is not appropriate for many forms of information processing relying on sensitive data. For example, using facial recognition information to identify known shoplifters or using biometric information for security, verification and authentication purposes. Another example of this is the use of biometric behavioral data to stop sophisticated attacks by automated bots which attempt to mimic human behavior. In order to stop these attacks, fraud prevention tools must rely on information about personal biological features. If consent were required to process the biometric data of the automated bots, then fraudsters might choose to decline consent to avoid detection by the fraud prevention tool.

CIPL recommends the NPC clarify that personal information processors can rely on the other bases for processing to process sensitive personal information, coupled with appropriate protections commensurate for the level of risk.

Recommendation: Clarify that Article 30 enables processing of sensitive personal information on the basis of all legal grounds for processing listed in the PIPL and that processing such information is not limited to the ground of consent.

Article 36: Access to Government Data

The PIPL states that State organs cannot disclose the personal information they process, unless otherwise provided for by laws or administrative regulations or if they obtain the consent of the individuals concerned. CIPL would like to highlight the importance of enabling government to business data sharing for important research, innovation and other purposes in the public interest.

Reasonable access to Government data is particularly important in China because a very large portion of useful data is controlled by the Government. For example, much personal credit data is controlled by the People's Bank of China and traffic-related data is controlled by the Ministry of Public Security. If access to such data is granted, analytics firms could help target lower automobile insurance rates and lower loan interest rates where appropriate, leading to benefits for Chinese consumers. The private sector could also use government data to build specialized application platforms for state, city and town government

organizations. For example, platforms to assist tax authorities in preventing tax refund fraud or to assist bank regulators with anti-money laundering efforts or enable traffic management authorities to improve congestion in local communities.

Recommendation: Revise Article 36 of the PIPL to provide for the sharing of government data for important research, innovation and other purposes in the public interest.

Article 38: International Transfers of Data

CIPL appreciates the PIPL's recognition that personal information may need to be transferred overseas for business needs. Article 38 of the PIPL permits the international transfer of personal information if the personal information processor meets one of the following conditions: (1) passes the security assessment organized by the Cyberspace Administration; (2) undergoes a personal information protection certification conducted by professional institutions in accordance with regulations of the Cyberspace Administration; (3) signs a contract with the overseas recipient; or (4) meets other conditions stipulated by laws, administrative regulations or the Cyberspace Administration.

Many organizations transferring personal information for business needs overseas will rely on the option of signing a contract with the overseas recipient that stipulates the rights and obligations of both parties and supervising the recipient's personal information processing activities to ensure the standards stipulated in the PIPL are met.

CIPL recommends clarifying the scope of supervision required to ensure the recipient of personal information meets the standards enumerated in the PIPL. This could be achieved by way of guidance by the Cyberspace Administration that stipulates that appropriate supervision includes conducting due diligence before entering into a contract with the overseas recipient, making clear within the contract the purpose of the transfer and the responsibilities of the receiving party, and taking appropriate action if the sender of personal information discovers that the recipient is acting in breach of its contractual obligations.

Moreover, it is not clear what is involved in order to pass the security assessment organized by the Cyberspace Administration or undergo personal information protection certification by professional institutions. Such matters should be clarified as a matter of priority in advance of or immediately following the passage of the PIPL. For example, China has endorsed the APEC Cross-Border Privacy Rules (CBPR) system[8] in 2011 and, as an APEC economy, would be eligible to seek active participation in this cross-border transfer certification. It would be useful to clarify whether the certifications referenced in Article 38 could enable potential future participation by China in the APEC CBPR system. In addition to enabling cross-border transfer certification, the PIPL should also enable codes of conduct and corporate rules for the same purpose, as other major new privacy laws or legislative proposals have done, such as the EU GDPR (i.e. GDPR codes of conduct and Binding Corporate Rules) and the Indian Proposed Personal Data Protection Bill (i.e. codes of practice and intra-group schemes).

[8] APEC CBPR, available at https://cbprs.blob.core.windows.net/files/CBPR%20Policies,%20Rules%20and%20Guidelines%20Revised%20For%20Posting%203-16.pdf.

Recommendation: Clarify the scope of supervision required by the personal information processor to ensure a recipient of personal information meets the standards of protection enumerated in the PIPL. Explain what is involved in order to pass the Cyberspace Administration's security assessment and to obtain personal information protection certification by professional institutions. Further, clarify whether the certifications referenced in Article 38 could enable China's participation in the APEC CBPR and add codes of conduct and corporate rules to the available transfer mechanisms in the PIPL.

Article 39: Consent for International Transfers of Data

If a personal information processor transfers personal information overseas, Article 39 of the PIPL requires it to inform the individuals of the identity and contact information of the overseas recipient, the processing purpose and method, the type of personal information to be processed and the way in which the individuals can exercise their rights over the recipient. The personal information processor must also obtain the separate consent of individuals to make the transfer of personal information.

Firstly, CIPL would like to highlight that the requirement to obtain an individual's consent alongside the requirements outlined in Article 38 of the PIPL is an outlier among data protection laws globally and will seriously impact the ability of organizations to transfer data abroad for legitimate and beneficial purposes.

The key concerns with requiring consent in addition to the other requirements are:

- Consent does not add additional protection to individuals. The security assessment, personal information protection certification, contract with the receiving party or other requirements stipulated by Chinese law, administrative regulations or the Cyberspace Administration are designed to provide robust protection to individuals in the first instance. In fact, such mechanisms impose more requirements on data recipients and provide more protection than consent as consent simply gives individuals a choice to accept whatever risk they are presented with.

- Requiring consent sends a confusing and inappropriate message about transfers to individuals. Asking for consent for all cross-border transfers could mislead people to think there is something inherently wrong or risky with such transfers. In the modern digital economy, transfers are essential to the provision of a wide range of products and services for consumers.

- Requiring consent imposes an unnecessary burden on individuals. Asking individuals to consent to every transfer of personal information would dramatically increase the number of consent requests they receive, overburdening them and having the effect of diluting and undermining the effectiveness of consent in situations where it might be meaningful.

- Requiring consent imposes an unnecessary burden on personal information processors. In preparing for compliance with the PIPL, organizations would have to implement the mechanisms and procedures associated with obtaining consent for transfers of personal information. This could cause substantial costs to new and existing businesses, and disruption to organizations that already have established mechanisms in place for the transfer of personal information across borders in line with common approaches found in many global data protection laws.

- Obtaining consent for every transfer of personal information is not always feasible. In some cases, it may be impossible to obtain consent for a transfer of personal information due to an organization's lack of relationship with, and/or contact information of, an individual whose personal information is being transferred.

In addition to the concerns raised above, it is important to highlight that, internationally, countries have steered away from requiring consent for the cross-border transfer of personal information. For example, the GDPR only allows the use of explicit consent as a basis for transfer in cases where a transfer cannot be made pursuant to an adequacy decision or an appropriate safeguard and the individual has been informed of the possible risks of the transfer. Under the GDPR, consent is a derogation from the general rules on overseas transfers. Moreover, in Canada, the Office of the Privacy Commissioner of Canada (OPC) conducted a public consultation in 2019 on changing its policy position for transfers to require consent for transborder data flows. At the conclusion of the consultation, the OPC ultimately decided that consent for transfers is not required and that the existing approach based on accountability remains appropriate.

Moreover, as mentioned above, China is part of APEC, has helped develop and endorsed the APEC Privacy Framework, and has helped develop the APEC Cross-Border Privacy Rules system. One of the core objectives of the APEC Privacy Framework is to ensure the free flow of data in the Asia-Pacific region and to promote "effective privacy protections that avoid barriers to information flows".[9] The Framework specifically calls out the role of the CBPR in furthering both privacy and maintaining information flows among APEC economies and with their trading partners, as well as in encouraging organizational accountability with respect to personal information.[10] Indeed, one of the foundational premises of the Framework was to create "conditions, in which information can flow safely and accountably, for instance through the use of the CBPR system". According to the Framework, the CBPR system was created so that "individuals may trust that the privacy of their personal information is protected" no matter where it flows.[11] An APEC Privacy Framework[12] section specifically on cross-border transfers provides as follows:

- *70. Any restrictions to cross border flows of personal information should be proportionate to the risks presented by the transfer, taking into account the sensitivity of the information, and the purpose and context of the cross border transfer.*

Further, it is noteworthy (but not surprising) that the program requirements of the APEC CBPR do not provide for choice or individual consent with respect to cross-border data transfers. Such an option would be inconsistent with APEC's and the CBPR's premise of providing accountability-based protections to the information regardless of geographic location.[13]

---

[9] See, for example, APEC Privacy Framework at Foreword and Preamble, paragraph 4, available at https://www.apec.org/-/media/APEC/Publications/2017/8/APEC-Privacy-Framework-(2015)/217_ECSG_2015-APEC-Privacy-Framework.pdf.

[10] *Id*. at Preamble, section 8.

[11] *Id*. at Part IV, B, III, paragraphs 65 and 67.

[12] *Id*. at Part IV, B, IV paragraphs 69 and 70.

[13] There is one limited exception to this. The Framework's accountability principle (Part III, principle IX, para. 32 plus Commentary) provides that where personal information in a domestic or international transfer cannot be protected through exercise of due diligence or other reasonable steps, an organization should obtain consent "to assure that the information is being protected consistent with these principles". However, this would not be the

China's proposal to introduce a consent requirement, therefore, is inconsistent with the goals of the Framework and the specific purpose and requirements of the CBPR: to make geographic location of personal information irrelevant because protections should flow with the information regardless of where it goes. Given that under the PIPL's proposed transfer framework sufficient protections and appropriate measures already exist, and given that a consent requirement addresses no additional risks nor adds protections, such additional obstacle to cross-border transfers is not warranted.

While the APEC Privacy Framework and the CBPR explicitly do not prohibit domestic privacy protections that go above and beyond what is provided by APEC, implementing a new requirement so at odds with the very premise of the APEC Privacy Framework and the CBPR warrants careful consideration. Part of the promise of the CBPR, which China someday might join, is to harmonize privacy and data protection practices across the APEC region (and maybe even beyond). This will be one of the principal benefits and incentives for organizations that certify to the CBPR. Any unnecessary national deviation, therefore, has the potential to directly undermine this harmonization benefit and, thus, the relevance and effectiveness of the CBPR in the long run.

As a result of these factors, CIPL recommends that the NPC remove the requirement to obtain separate consent on top of the requirements listed in Article 38 to transfer personal information overseas.

In addition, Article 39 requires that personal information processors provide individuals with the identity and contact information of the overseas recipient and the way in which the individuals can exercise their rights over the recipient. With respect to the contact information and identity of third parties, it is important that the NPC consider the scale of international transfers that take place on a daily basis. Providing each individual with the specific contact information and identity of each third party recipient may be extremely burdensome and potentially impossible depending on the nature of the transfer and the relationship of the personal information processor with the individual.

Furthermore, with respect to rights, individuals should exercise all rights requests through the organization that originally collected their information. Third parties that receive rights requests from individuals they have no immediate relationship with would be required to verify that they did in fact receive information about the individual from another organization. This may be impossible to verify as the organization may have received information from hundreds of different organizations and depending on the type of data transferred, it may be impossible to link the individual to the specific information received. CIPL recommends revising Article 39 to remove the requirement that personal information processors provide information on how individuals can exercise their rights against a third party to which it transfers personal information. In communicating with individuals, the focus should be on how they can exercise their rights against the personal information processor who can follow up with the third parties it transferred the information to if required.

Recommendation: Revise Article 39 to remove the requirement to obtain separate consent on top of the requirements listed in Article 38 to transfer personal information overseas. Remove the requirement to

context under the CBPR or any mechanism whereby the transfer of personal data occurs subject to appropriate accountability measures that ensure continued protection at the appropriate level.

provide information about the contact details of overseas recipients of personal information as well as information about how to exercise rights against such entities.

Article 40: Cyberspace Administration Security Assessment

One of the options for transferring personal data overseas listed in Article 38 is the completion of a security assessment organized by the Cyberspace Administration in accordance with Article 40 of the PIPL. Article 40 requires that critical information infrastructure operators and personal information processors that handle personal information up to the amount specified by the Cyberspace Administration shall store within China the information they collect and generate within the territory. Article 40 notes that if it is necessary to transfer such personal information overseas, such entities must pass the security assessment.

CIPL understands that certain forms of information are required to be stored locally within a country for public interest and national security purposes. However, CIPL cautions against any form of data localization in a privacy law. Given the global nature of the digital economy, CIPL believes that countries should enable the free flow of personal information while ensuring the protection of such information through organizational accountability and sensible data transfer mechanisms. One clear example of this in the PIPL is the ability for organizations to transfer personal information overseas through the use of contracts that stipulate the rights and obligations of both parties. Requirements to store personal information locally can have the following consequences:

- They prohibit the use of technologies that rely on global and distributed networks, such as data analytics, cloud computing and AI and machine learning applications.

- They impose the creation of redundant storage systems. International organizations operating in China would be required to create redundant storage systems in China to store data which would raise costs, disrupt business processes and create information security risks.

- They increase costs to prohibitive levels for local and foreign small and medium enterprises. New market entrants may be unable to take advantage of competitive cloud computing services that allow them to enter the market and compete with larger organizations. Foreign enterprises may not have the capital to set up redundant storage systems in China, which effectively blocks them out of the market and prevents their ability to serve Chinese consumers.

- They compromise data security. Requiring the concentration of personal information in China prevents organizations from partitioning data across global servers, which can provide an additional layer of protection against hackers and business continuity in the case of natural disasters.

Given the above consequences, CIPL recommends that the Cyberspace Administration carefully define the amount of personal information that an organization must process in order to trigger the requirements of Article 40. The amount should be substantial to avoid imposing a data localization requirement on almost all organizations. In calculating a reasonable amount, the population and number of internet users should be considered.

Moreover, CIPL recommends that the PIPL provide an exception for intra-company transfers, including the transfer of employee related information, outside of China by global companies that trigger the Article 40 security assessment requirements. Such transfers are necessary for day-to-day operations and would promote increased investment in China as organizations would not have to create completely separate business entities to engage in the Chinese market.

Finally, it is important that the requirements of the security assessment are consistent with China's Cybersecurity Law to ensure certainty and coherence for organizations.

Recommendation: Carefully define the amount of personal information that triggers the Article 40 security assessment requirements. Provide an exemption for intra-company transfers, including the transfer of employee related information, outside of China by global companies meeting the thresholds of Article 40. Ensure that the requirements of Article 40 are in line with those contained in China's Cybersecurity Law.

Article 42: Consequences for Foreign Personal Information Processing Activities Resulting in Harm to Individuals

Article 42 of the PIPL notes that where foreign organizations or individuals engage in personal information processing activities that harm the personal information rights and interests of Chinese citizens or endanger the national security or public interests of the State, the Cyberspace Administration may put such organizations or individuals on a list limiting or prohibiting personal information provision, issue a warning, and adopt measures such as limiting or prohibiting the provision of personal information to them, etc.

It is currently not clear what action an organization will have to take following such a determination where it has already provided personal information to the foreign organization. CIPL recommends the PIPL outline if the organization's obligation is to simply comply with the measures specified by the Cyberspace Administration or if it must take specific remedial actions. This can assist organizations in assessing their risks and obligations before making transfers of personal information.

Recommendation: Outline the actions organizations that have transferred data to an overseas entity are required to take following measures implemented by the Cyberspace Administration against foreign personal information processors that have engaged in harmful processing under Article 42.

Article 43: Corresponding Measures against Other Countries and Regions

The PIPL states that where any country or region adopts discriminatory prohibitions, restrictions, or other similar measures against the People's Republic of China in respect of personal information protection, the People's Republic of China may take corresponding measures against the country or region in light of the actual situation.

While these are valid concerns, CIPL believes that such measures are typically the subject of political and bilateral trade discussions and do not speak to the obligations of organizations or the rights of individuals under the PIPL. Moreover, such a provision, which is not typically articulated in personal information protection laws, runs the risk of undermining the sense of legal certainty a data protection law such as this one should create for organizations, both with respect to general compliance and cross-border data

transfers. CIPL recommends removing Article 43 from the PIPL and addressing such matters via other avenues.

Recommendation: Remove Article 43 from the PIPL.

Article 47: The Right of Deletion

The PIPL provides individuals the right to request the deletion of their personal information in certain circumstances. This includes if the individual withdraws consent.

It is important to recognize that withdrawal of consent leading to deletion of data can be highly problematic in certain contexts. For example, in the medical research context, if an individual withdraws consent to processing for a clinical trial, the removal of their information from the results of the trial may impact the outcome of the trial for wider society. CIPL recommends that the PIPL provide for such scenarios and make clear that Article 16 (the right to withdraw consent) only applies with respect to the right of deletion where the retroactive deletion of data is possible and does not frustrate the overall processing operation for which the data was originally used. If it would frustrate the processing, restriction of further processing of the data may be possible as an alternative.

Recommendation: Clarify that the right to deletion by virtue of withdrawing consent only applies where retroactive deletion of data is possible and does not frustrate the overall processing operation for which the data was originally used. In cases of frustration of processing, restriction of further processing rather than deletion as an alternative may be possible.

Article 51: Obligation to Appoint and Register a Personal Information Protection Officer

Article 51 of the PIPL notes that a personal information processor who processes personal information up to the quantity specified by the Cyberspace Administration shall appoint a person in charge of personal information protection to supervise personal information processing activities, protection measures taken, etc. In addition, the personal information processor must disclose the name and contact information of that person, and report that information to the relevant authorities.

This is similar to the requirement set out in the Personal Information Security Specification, which entered into force in October 2020 and requires the appointment of an in-house personal information protection officer where an organization processes or expects to process the personal information of more than 1,000,000 individuals or processes sensitive personal information of more than 100,000 individuals.[14] To ensure consistency between the PIPL and the Personal Information Security Specification, CIPL recommends that the same thresholds apply for the appointment of a personal information protection officer under the PIPL.

CIPL cautions against a requirement to disclose and register the contact information of the individual with the relevant authorities. This would add an undue burden and unnecessary costs to organizations that would have to update the registration every time an employee left, and a new personal information

[14] See Article 11.1(b), Specifying responsible department and person, Information security technology – Personal information security specification, National Standard of the People's Republic of China, GB/T 35273-2020.

protection officer is appointed. Rather, the organization should be required to register that it has in fact appointed a personal information protection officer and keep this representation up to date.

Recommendation: Revise the requirement to disclose and register the contact information of the personal information protection officer to the relevant authorities and only require registering whether such an officer has been appointed and keeping such representation accurate and up to date. Align the thresholds triggering the requirement to appoint a personal information protection officer with those under the Personal Information Security Specification.

Article 52: Obligation to set up a specialized agency or appoint a representative

Article 52 of the PIPL requires that a personal information processor outside the territory of China set up a specialized agency or appoint a representative within the territory of China to handle matters concerning personal information protection, and report the same to the relevant authorities performing personal information protection duties.

With respect to setting up a specialized agency, CIPL recommends the NPC clarify that such an agency can include one of the organizations affiliate companies.

Regarding appointing a representative, CIPL recommends that the PIPL include specific exemptions to this requirement. For example, under the GDPR, there is no requirement to appoint a representative where the processing is occasional, does not constitute processing sensitive information on a large scale and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing.

Recommendation: Clarify that an organization's affiliate company can serve as a specialized agency for the purposes of Article 52. Add exemptions to the requirement to appoint a representative within China in line with those found in other privacy laws, such as the GDPR.

Article 53: Obligation to conduct audits

The PIPL requires a personal information processor to conduct audits on a regular basis to determine whether its processing activities and protection measures comply with the provisions of laws and administrative regulations. Article 53 also provides that relevant authorities performing personal information protection duties may direct personal information processors to engage specialized entities to carry out such audits.

CIPL recommends that the PIPL require the relevant authorities to provide a personal information processor with reasonable and sufficient notice that it is required to engage a specialized entity to carry out the audit. There may be internal processes that need to be completed before engaging a new entity and providing access to systems, policies, controls and sensitive business information. As a result, organizations may need some time to prepare in advance of the audit taking place.

Recommendation: Add a requirement for the relevant authorities to provide reasonable and sufficient notice to organizations to engage a specialized entity to carry out an audit.

Article 54: Advanced Risk Assessment

The PIPL requires a personal information processor to conduct a risk assessment in advance of the following processing activities: (1) processing of sensitive personal information; (2) using personal information for automated decision-making; (3) entrusting any other person with processing, providing personal information to any third party or disclosing personal information; (4) transferring personal information overseas; or (5) other personal information processing activities with a significant impact on individuals.

It is important to highlight that organizations engage in millions of processing activities along the lines of those listed in Article 54 daily. It would be impossible for organizations to carry out a full-blown risk assessment for every single one of those operations in advance. CIPL believes that organizations should be permitted to engage in an initial risk pre-screening of their processing activities and only be required to carry out a full-blown risk assessment in cases where the screening or preliminary risk assessment indicates that the processing is likely to result in a high risk to individuals. Imposing a requirement to carry out a *full* risk assessment in advance of all data processing is not something that businesses can effectively operationalize. A pre-screening or preliminary risk assessment will be able to remove many no- or low-risk information processing activities from the requirement of a full-blown risk assessment.

Moreover, in the context of transferring personal information to overseas third parties, organizations already have to comply with the requirements contained in Chapter III of the PIPL, which makes the requirement of conducting a further risk assessment redundant. With respect to processing activities that have a significant impact on individuals, it is not currently clear what constitutes a "significant impact" under the PIPL. The Cyberspace Administration should provide clear guidance on the types of processing that may produce significant impacts which can be rebutted via the risk assessment carried out by the organization. This would add some clear parameters and guideposts as to when such risk assessments would be required to be conducted.

Recommendation: Clarify that conducting an initial pre-screening of the processing activities listed in Article 54 and carrying out a full-blown risk assessment if such a screening indicates a high risk to individuals would be sufficient to meet the Article 54 requirement to conduct advance risk assessments.

Article 55: Breach Notification

Article 55 of the PIPL requires a personal information processor to immediately take remedial measures following the identification of a data breach and notify the authorities performing personal information and protection duties and individuals of the breach.

Currently, the PIPL does not provide a harm threshold for the notification of data breaches to the authorities. For individuals, notification is not required if the personal information processor has taken measures to effectively avoid damage caused by the breach. As a result, personal information processors would have to notify all breaches without distinction to the relevant authorities. This could lead to over-reporting by organizations and a risk of notification fatigue and an undue burden on the authorities. CIPL recommends that the NPC add a qualification in the PIPL whereby only those personal information leaks or breaches that are likely to result in harm or risks to individuals need to be notified to the relevant

authorities. For notification to individuals, CIPL recommends either the same or a higher threshold (as is common in other privacy and breach notification laws).

In addition, the timing of the notification is not clear in the PIPL. Identifying an appropriate timing obligation is a crucial challenge for lawmakers seeking to balance the risk associated with inappropriate delays against rushed notifications. On the one hand, a delayed notice could prevent affected individuals from receiving actionable information about the risk to their data and steps they may take to protect it. Alternatively, a rushed notification increases the likelihood that organizations will not have sufficient information about the nature and scope of the issue and will provide notice prematurely. This will have negative results for both the affected individuals and the relevant organization.[15] Currently, the Draft Law states that notification must take place immediately following the identification of a data breach. In practice, compliance with this requirement would be impractical. Organizations need time to ascertain how the breach occurred, understand the severity of the breach, potentially conduct a forensic investigation through hiring outside expertise, understand what action must be taken internally to restore the reasonable integrity of the affected system, gather all the relevant facts for the reporting, etc. This can take many days, if not weeks, to complete. CIPL recommends that the PIPL require that notice be provided in the most expedient time possible and without unreasonable delay but not later than a specified number of days (e.g., 30 or 45 days) after the entity becomes aware of a data breach. This requirement suggests that the timeframe to notify would begin when the entity either (1) determines that a breach has occurred or (2) is notified (e.g., by law enforcement or a service provider) that a breach occurred.[16]

Recommendation: Add and elevate the harm thresholds that trigger the notification requirement to report a breach to the relevant authorities and individuals respectively, in Article 55. Revise the requirement to notify breaches from "immediately following identification" to the most expedient time possible and without unreasonable delay but not later than a specified number of days (e.g., 30 or 45 days) after the entity becomes aware of a data breach.

Article 58: Duties of the Authorities

Article 58 of the PIPL notes that the Cyberspace Administration shall, according to their respective duties and powers, advance the building of a socialized service system for personal information protection. It is not currently clear what is meant by such a system or what would be required of companies with respect to such a system.

CIPL recommends that the Cyberspace Administration explain that advancing such a system would entail the holding of a public consultation to obtain stakeholder input and explain the system before it becomes effective.

[15] Seeking Solutions: Aligning Data Breach Notification Rules Across Borders, Hunton Andrews Kurth and the US Chamber of Commerce, 2019, available at https://www.huntonak.com/en/insights/seeking-solutions-aligning-data-breach-notification-rules-across-borders.html.
[16] *Id*.

Recommendation: Clarify that advancing a socialized service system for personal information protection involves conducting a public consultation on the proposed service to explain the system and gather stakeholder input.

Article 62: Liability and Fines

Article 62 of the PIPL states that where personal information is processed in violation of the law or without any necessary security protection measures in compliance with regulations, the authorities performing personal information protection duties shall order a correction, confiscate any unlawful income and issue a warning. If corrections are not made, fines may be imposed on organizations of up to 1 million RMB. Article 62 further notes that if the unlawful act is "grave", authorities can impose a fine of up to 50 million RMB or 5% of last year's annual revenue, among other actions.

CIPL appreciates that the first level of fines are in line with Article 64 of the Chinese Cybersecurity Law for unlawful acts infringing personal information. With respect to the second level of fines, it is not clear what constitutes a "grave" unlawful act. CIPL recommends that the NPC clarify the definition of such an act in the next iteration of the PIPL. With respect to the amount of the fine for a grave unlawful act, it is not clear in which instance the fine will be a monetary amount up to 50 million RMB or 5% of revenue. It would be helpful to clarify (1) the circumstances in which the fine will be a set monetary amount or a percentage of revenue and (2) that the revenue in question relates to revenue in China.

The PIPL also imposes liability on any person in charge or other directly liable individual for unlawful and grave unlawful acts infringing personal information. CIPL believes that natural persons acting in their official capacity on behalf of a legal person that employs them should not be personally liable for violations of the law, unless they are top officers or directors and have acted willfully or with gross negligence and for the purpose of financial or similar gain. Imposing criminal liabilities for such violations on individuals, especially internal data privacy experts/personal information protection officers would undermine the ability of organizations to find qualified information protection officers and similar staff responsible for the handling of personal data and, thus, undermine the goals of this law. Therefore, CIPL recommends clarifying that any person in charge or other directly liable individual refers to top company officers or directors who acted willfully or with gross negligence for financial or similar gain and not simply in violation of the law as this would also include lower level violations and any negligent act.

Recommendation: Clarify what constitutes a "grave" unlawful act under Article 62. Clarify, for such acts, when the fines will be a set monetary amount or percentage of revenue and that the revenue in question relates to revenue in China. Clarify that personal liability under Article 62 applies only to top company officers or directors who acted willfully or with gross negligence for financial or similar gain.

Article 63: PIPL Infringement Impact on Credit Files

Article 63 of the PIPL states that any unlawful act under the PIPL shall be entered into credit files as required by relevant laws or administrative regulations, and be disclosed to the public. CIPL does not see a link between PIPL violations and credit risks. CIPL recommends deleting Article 63 and dealing with any penalties for infringement within the remit of Article 62 and related articles.

Recommendation: Remove Article 63 from the PIPL.

Article 69: Definitions

Article 69 defines "personal information processor" as any organization or individual that autonomously determines the processing purpose, processing method or any other matter relating to the processing of any personal information. Unlike other data protection laws, the PIPL only seems to reference the obligations of personal information processors, which are known as data controllers in some other privacy laws. However, there are also other actors involved in the processing of personal information, including third party service providers. For example, cloud service providers, payroll processors, etc. The PIPL does not elaborate on the obligations of such entities and it is unclear to what extent they are covered by the PIPL. CIPL recommends clarifying the role of third party service providers in relation to personal information processors in the PIPL.

Moreover, as a matter of drafting, it is advisable that the NPC replace the term "personal information processor" with the term "personal information controller". Third party service providers are commonly referred to in other jurisdictions as "data processors" and CIPL recommends including the term "personal information processor" in reference to such service providers. These are globally accepted terms and their inclusion will ensure consistency not only on a global scale as Chinese organizations interact in the global economy but also on a domestic scale as the Personal Information Security Specification refers to a "personal information controller".[17]

In addition, Article 69 defines "anonymization" as the process of handling personal information in ways that make it unable to identify a specific natural person or be restored to its original state. This is a very high standard to meet as nothing is completely irreversible. CIPL believes the NPC should clarify in Article 69 that data should be excluded from the scope of this law when individuals are not identified, having regard to all means reasonably likely to be used, by the personal information processor or any other person, to identify the individual. This more realistic standard provides an incentive for organizations to anonymize data using measures appropriate to the risk of identification, which can be assessed through appropriate risk assessment processes for a specific context. When this is coupled with procedural, administrative and legal protections against de-anonymization (e.g. internal accountability measures and a commitment of organizations not to re-identify data; enforceable contractual commitments with third parties not to re-identify data; and legal prohibitions on unauthorized re-identification by any third party), individuals are effectively protected.

Moreover, this revised standard is in line with Article 24 of the PIPL which states that if a personal information processor provides anonymized information to a third party, the third party may not use technical or other means to re-identify individuals. Under the original definition of anonymization, such a risk would be impossible, as data would be unable to be restored to its original state or identify a specific individual. Thus, CIPL believes the standard proposed above is more consistent with the rest of the PIPL.

Recommendation: Clarify the role of third party service providers under the PIPL and use more standardized and globally recognized terms, such as "personal information controller" (in reference to personal information processors) and "personal information processor" (in reference to third party

[17] See, generally, Information security technology – Personal information security specification, National Standard of the People's Republic of China, GB/T 35273-2020.

service providers) throughout the PIPL. Revise the definition of anonymization to reflect the more realistic standard of reasonable anonymization coupled with procedural, legal and administrative safeguards.

Article 70: Entry into Force

Although the current draft is silent as to the exact day, month and year the law will enter into force, CIPL recommends that organizations are given ample time to comply with the PIPL and no less than two years from the date the PIPL is passed. This is consistent with other privacy laws globally, including the GDPR and the Brazil LGPD.

Recommendation: Specify in Article 70 that organizations will have two years from the date the PIPL is passed to be fully compliant with the law.

Conclusion

CIPL is grateful for the opportunity to provide input to the Standing Committee of the National People's Congress of the People's Republic of China on the Draft Personal Information Protection Law. We look forward to future opportunities to comment on and provide input into this process.

If you would like to discuss any of the comments in this paper or require additional information, please contact Markus Heyder, mheyder@huntonAK.com, Sam Grogan, sgrogan@huntonAK.com or Dora Luo, doraluo@huntonAK.com.